Version number attack isolation technique for internet of things

[1]Hiral Patel, [2]Hiren Patel, [3]Bela Shrimali

[1]Research Scholar, [2]Professor, [3] Assistant Professor
[1]Master of Computer Engineering Department,
[1]LDRP Institute of Technology and Research, Gandhinagar, Gujarat, India.

Abstract : The Internet of things (IOT) is the dynamic network that uses IPv6 Routing Protocol for low power and lossy networks (RPL) between participated nodes. The RPL routing protocol optimized network topology, the RPL applies the version number and rank into the constrain network. However, an intruder can mutate and diffuse version number into low power and lossy network (LLN) to reduce network lifetime known as version number attack. This attack will impact the network by increases in end-to-end delay, energy consumption, packet loss ratio (PLR) and decries throughput and packet delivery ratio(PDR) etc. In this work, the novel methodology is proposed for the isolation of version number attack based on threshold and monitor mode techniques. The proposed methodology is implemented in Ns2 and results are compared with existing method based on the parameter viz. The results depict that the proposed work is efficient to handle version number attack.

Index Terms **– Version number, RPL, Threshold, Monitor mode.**

I. INTRODUCTION

Internet of things (IOT) is a network of corporal entities. It is an arrangement of numerous types of equipment like sensors, activators, mobile entities, and many more, which are interconnected with the help of internet. These entities interact and share information with each other. This communication and sharing of information have relied on predetermined routing protocols for the attainment of elegant restructuring, deployment, detection, private genuine online observation, online advancement, procedure systemization, management etc. Internet of things may be divided into three category [1]: (1). Public to public, (2) Public to instrument /entities, (3) Entities /Instrument to equipment /instrument, communication via the internet. These physical objects and entities of IOT are communicate and collaborate with the help of exclusive addressing systems, for the development of novel functions, services and attain ultimate objective [2]. These communication and collaboration between entities use network layer standard routing protocol called RPL [3].

The architectural design of RPL is a collection of numerous Destination-Oriented Directed Acyclic Graph (DODAG) systems. In this scheme, every DODAG considers several wireless sensor equipment which are connected via a DODAG path. For the differentiation of all the DODAGs present in the system, RPL instance ID; DODAG ID; DODAG version number; and rank values are utilized/used. For the establishment and maintenance of DODAG and also for the direction finding, novel ICMPv6 control messages like DIO (DODAG Information Object), DIS (DODAG Information Solicitation), DAO (Destination Advertisement Object) and DAO-ACK (Destination Advertisement Object Acknowledgement) are used by RPL [3][4][5].

The implementation of DODAG topology is initiated by the DODAG sink node. The structuring of message forwarding paths is performed by the launching of DIO information. After the retrieval of DIO information, the associated nodes are informed with the help of onward upgraded data in the subsequent DIO. Every node in DODAG contains a grade which shows the location of a sensor node with respect to other associative nodes and also towards the DODAG root [4] [5]. In the last phase of the routing process, the sensor node chooses a favored relative which is included in the parent list and this also becomes a default entry. While a node desires to onward information through the DODAG path, the node firstly attempts to propel the message to the favored relative or parent. During the failure of message broadcasting, the message is transferred to any of the non-favored relatives subsequently. For the optimization of system assets, RPL utilizes the trickle approach in spite of transferring DIO periodically. This process is used for transferring the messages occasionally. Every node in the network using RPL are permitted to select the data packets path either in ascending or descending to forward it to the next neighbor node [6]. Non-storing mode or storing mode is effectively providing support to descending steering. For the prevention of loop structuring, the grade value is utilized by RPL. The parent nodule should always have a lower rank in comparison with its children. While DODAG does not remain acyclic, at that time DODAG loops may emerge. In order to prevent this, the sub-DODAG is poisoned by its parting nodule. This is performed by the advertisement of an inestimable rank. During the recognition of discrepancies, revamp method is launched by RPL. Mainly two types of revamping methodologies are accessible in RPL. These are known as universal (global) and confined (local) repair methodologies [5].

However, the flexibility of the RPL mechanism enables a number of intrusion nodes to harm the network. A. Kamble et al. [7] addressed the security stiff challenges in the network of wireless sensors based on the various form of intrusion. They incorporated details about diverse attacks against the RPL protocol, characteristics of attacker activity and prevention systems.

II. A VERSION NUMBER ATTACK

The RPL protocol is considered susceptible to version number intrusion. The version number intrusion utilizes the universal revamp method for the overloading of the network. The root initiates a universal repair when too many inconsistencies are detected in the network. After the recognition of several discrepancies, a universal repair methodology is initiated by the path. This comprises the restructuring of complete DODAG with the help of version number increment [8]. The DIO message carries the version number. After receiving the DIO message via its parent, the message is compared with accessible version number besides the one who receives

it. The message about existing rank will be ignored if the obtained version number is higher in rank. In this case, the sensor node resets the trickle timer and starts a novel process for connecting the DODAG [5].

This universal repair system assures about a loop free structure but at the same time, this is expensive also. A prior value of the version publicized in DIO communication designate that the sensor node did not drift to the novel adaptation of DODAG [9]. Thus, this kind of sensor node should not be chosen favored parent node. During the period of universal repair, two editions of a DODAG repair may survive in the identical time slot. However, in order to avoid loops, information packages from the prior edition of revamp are permitted to transfer in the novel edition but not by other means. Because the junction (sink node) of the system has not been achieved, therefore the older edition no longer remains a DAG. In this scenario, loop-free frameworks cannot be assured. For the avoidance of promising discrepancies in the system, the version number should be broadcasted in an unaffected manner via DODAG. RPL does not include any mechanism for ensuring the truthfulness of version number in acknowledged DIO information. The attacker node can alter its value for harming the system. After receiving an attacker DIO with a novel version number, sensor nodules reset their trickle timer, revise the edition and promote this novel edition via DIO messages to their vicinity also. Because of this illegal version number may broadcast through the system. This kind of version number exploitations in DIO packages may be the reason for the needless restructuring of entire DODAG. This results in the generation of the loop in the system. Also, because the novel edition of DODAG is not manufactured from the root, the topology remains no longer acyclic and thus allows the loops to ensure [10]. This may pessimistically crash the power assets of nodes, steering of information packages and tunnel accessibility. The sensor node cannot recognize this intrusion locally. A malevolent DIO package approaching from a parent appears to be genuine for a nodule [11]. When this packet arrives from a child, in this case, the node considers that this is because of the discrepancy of the network. The localization of the malevolent DIOs resource is unfeasible from a merely restricted end. The interaction among nodes is necessary for finding the source of the intrusion.

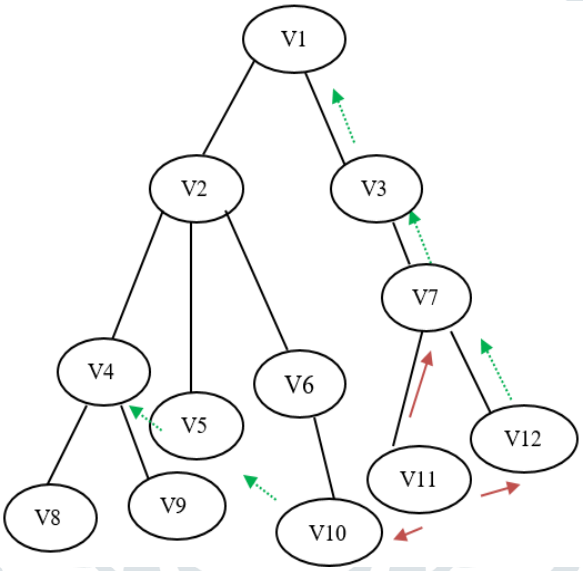

Figure 1. Representation of version number attack [12]

The figure 1 describes the different probabilities of sensor node with the help of topology. In order to illustrate figure 1, we provide situation of recognition policy under typical circumstances. In that situation, the intrusion is positioned at location v11; it propels DIO malevolent information to entire neighbouring area (bold red arrows) which is conveyed by other sensor nodules (dotted green arrows). The different monitoring nodes send details of this intrusion to the sink which is the conveyer of inappropriate information and their associates [12][13].

In the final stage, the possible intrusion catalog and the neighbors catalog are customized in the path observing nodes. Nodes v 07 and v 10 accept intrusion messages from intrusion v11 and transmit an information to the sink [14]. This message contains the irregular messages of attacker and their neighbors. Nodes v 04 and v 01 do the same with relays v 05 and v 03. After gathering the information, the localization process can be started by the sink for the establishment of intrusion and safe nodes catalogue.

In the beginning of potential attacker list, v11 is added to the intrusion catalog and the equivalent neighbors with no probable intrusion {v 03, v 06, v 12} are added to the secure catalog. Because, the second entry v11 is already in the intrusion catalog, only the secure catalog is rationalized with the associates of observing node v 10 which are v 05 and v 09. The third admission is v 03 which is already in the secure catalog, thus in this case, only secure catalog is rationalized with the equivalent associate v 02 [15]. The similar procedure is continued for the very last admission v 05 which is already included in the secure catalogue.

So, in this paper we claimed to efficiently handle version number attacked and try to reduce end-to-end delay, energy consumption and packet loss ratio. This paper is organized as follows. Section III present related work on detection of version number attack. Section IV present isolation technique of detection of version number intrusion node. Section V present evaluation of proposed technique. Finally, section VI present conclusion and future works.

III. LITERATURE REVIEW

The numerous research work have been studied and analyzed to understand the version number attack. Over previse work [16], we have disused the varies Intrusion detection technique (IDS) based on trust-based and non-trust-based for detection and prevention of version number attack. In this section, we have to focus on the detection of version number attack based on monitoring node techniques and trust-based technique.

A. Aris et al. [10] presented a deep study of RPL version number attacks. The investigation of the attacks was also performed which was based on different scenarios. The investigation was performed on a practical network topology containing both mobile and stationary nodes. These nodes contained a number of cardinalities. The research work was based on IETF routing requirements. The effect of the version number invasions on power utilization of the nodes was also calculated. A probabilistic approach was used for calculating the attacks probabilities. The results of performance were demonstrated according to the different values of p. The outcomes of the simulation depicted that the mobile attackers and the distantly placed nodes had almost the same effects on the network performance.

A. Mayzaud et.al [17] presented a novel classification approach for the categorization of the attacks found beside the RPL. For this approach, they have considered mainly three classes of attacks viz attack on resources, attacks on topology and, attacks on traffic. The lifespan of the network was reduced by the invasions against resources. These attacks generated a lot of false communication or constructed a number of loops. When the attacks were performed against the topologies, the network congregated to the suboptimal arrangement. The intruder node capture and the examined a wide part of the network in case of attacks. The researchers have proposed a lot of approaches for the prevention of these types of attacks based on different properties. The implementation and the management of the security modes were not mentioned by the RPL specification technique. Thus it was concluded that the transaction among different security levels was a major challenge for the accepted structure of RPL networks.

H.A. Abdul-Ghani et.al [18] proposed a new internet of things suggestion approach relied upon constructing blocks policy. This was basically a four-layered reference model. First, an IOT asset relied on invasion plane comprising of four mechanisms was presented. These components were software, information, protocol wrapping the entire IOT stack and substantial objects. Second, a pattern of IOT security aim was defined. The IOT invasion classification for every component was identified in the third layer. In the final layer, violation of security aims and the association among every attack was identified.

Z.A. Khan et al. [19] proposed some new approaches for IDS which were very suitable for the tiny devices. For managing the status information about the neighbors, they have used the faith management technique. They claimed that, the proposed approach proved very successful for singling out nastily behaving units. The presented approach was most suitable against the three types of RPL protocol attacks like sinkhole attacks, selective forward attacks and version number attacks.

A. Mayzaud et al. [20] proposed a method for the recognition of version number attacks presented in the networks of RPL after comparing a lot of presented internet of things observing solutions. Their proposed approach was based on a monitoring architecture named as distributed monitoring architecture. This architecture, in case of AMI infrastructures, conserved the inhibited node resources. For the identification of the intruder, the monitoring node association approach was utilized. After collecting the required recognition data from the all-observing nodes, the localization process was implemented by the root. A vast experimental evaluation carried out for evaluating the performance of the presented solution. It was found that by using strategic monitoring node replacement, the false positive rate could be reduced. The problem of scalability was also considered during the experiments.

H. Abdo et al. [21] proposed a novel approach for ensuring security and safety in case of industrial threat investigation. They have combined safety investigating system named bowtie analysis with the newly developed version of security analysis. The modified version was named as attack tree analysis. A comprehensive demonstration of the risk scenario was presented by the combination of the attack tree and bowtie analysis approach in terms of safety and security. The tested results showed that their method performed well.

IV. PROPOSED METHODOLOGY

The proposed work is based on the detection of version number attack on the Internet of things. The RPL is the routing protocol which is responsible to establish the path from source to destination with the use of version number. The path will be established to the destination which has a maximum version number. The malicious nodes enter into the network and reply to the source node with the maximum version number. The source is forced to an established path through a malicious node. In this research work, the novel approach is designed for the detection of version number attack to achieve previously defined goals like delay reduction and efficiently energy consumption.

In the proposed methodology, the delay of each node is calculated on the basis of distance, it means that for this distance this much will be the delay. The delay is calculated from one node to all other nodes in the network. The technique of monitor mode is applied in which every node watch activities of its adjacent node. The node which has maximum delay will be detected as the malicious node from the network. To isolate the malicious node from the network, the technique of multipath routing is applied in the network. However, a malicious node is removed by the base station using global repair operation in novel RPL protocol. Due to the lack of compatibility of RPL in NS-2, we applied the multipath routing technique for isolation of malicious node. The proposed methodology is based on the concept of threshold value and monitor mode. Following are the various steps which is applied for the detection of malicious nodes from the network:-

1. The cluster network is deployed with the finite number of sensor nodes

2. The malicious node increases the value of version number and source select path through the malicious node

3. The expected delay is calculated by equation number 1 during network creation

$$\text{Delay} = \text{Time to live} * \frac{Summation\ of\ distance\ between\ \ each\ \text{intermediate sensor}\ nodes}{Distance\ between\ source\ and\ destination} \quad (1)$$

The distance between the sensor nodes is calculated with equation number 2 [22]

$$\text{Distance} = \big(a(x+1) - a(x)\big)^2 + \ (a(y+1) - a(y))^2 \quad (2)$$

Where, x and y is the representing graphical position/coordinates of particular node in network.

The predicted delay is also calculated with equation number 1 during successfully receiving the data packet at the destination node.

4. If delay in the network increased, participation nodes in the particular path starts to monitoring the delay of adjacent node into the network to detect the malicious node in the path. That process is known as node localization technique.

5. After malicious node detection, the path without malicious will be selected using multipath routing [23]. The selected path will be checked for the malicious node if present then multipath routing will be used for new path. The procedure is continued until the selection of a secure path

6. Data packets will be transfer from source to destination in all cases

Role of cluster head is to pass all cluster member information to the base station. In the proposed algorithm, energy and distance of every node is taken into consideration to identify a cluster head. The node with maximum energy and minimum distance from the base station is taken as the cluster head, as shown in algorithm 1.

Algorithm 1:

Cluster head creation (n) // n = total number of sensor nodes

1. set a = $\frac{n}{10} + 1$ // a = 10:1 ratio used for selection of number cluster head
2. set node[p].distance = 800;
3. set node[p].energy = 0;
4. for (j = 0; j < a; j++) do // for each cluster in the network
5. for(i = 0; i < n; i++) do //for every node in the cluster
6. if(node[i].distance < node[p].distance && node[i].energy > node[p].energy) then
7. node[j] = node[i];
8. p = i;
9. end if
10. end for
11. end for

V. EXPERIMENTAL EVALUATION

Experimental Test beds:

The proposed technique is based on the threshold and monitor mode techniques for the isolation of malicious nodes from the network. The proposed technique is employed in network simulator version 2 (ns-2) by considered various parameters described in table 1. Ns-2 is a very popular and open-source tool for designing of contrasts scenarios with different protocols and without equipment cost. So we have chosen ns-2 for implementation and analyses of the result.

Table 1: Simulation Parameters

Parameter	Value
Area of network	800 * 800 meters
Total number of network nodes	38
Sink node	1
Number of attacker node	1
Antenna type	Omi-directional
Queue type	Priority queue
Simulation time	14 second
Traffic type	CBR
Data Rate	250 kbit/ second

Results and Comparisons:

Our algorithm is evaluated in ns-2 with the descried parameters, experiments are evaluated for ten times and average results are used for the analysis and comparisons with the existing trust based intrusion detection system (TIDS) [19]. It have been identify over proposed technique is performed well compare to the existing one. The existing approach is compared based on end-to-end delay, energy consumption, throughput, PLR and PDR. These are the criteria or parameter used to measure network parameters. Also the devices used in communication are battery based and their performance and participation depends on energy consume by them. And hence, energy consumption are consider for comparisons.

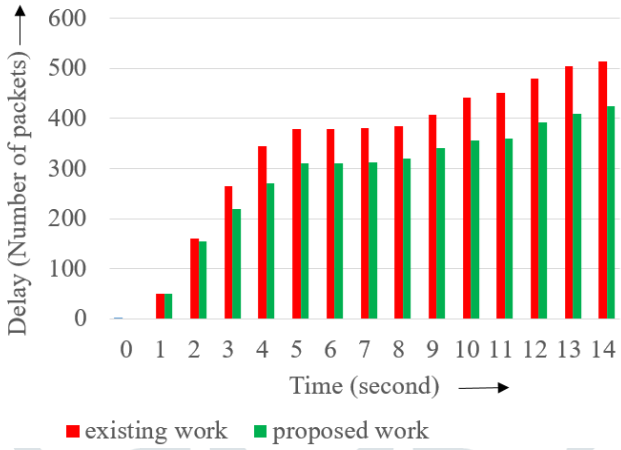

Figure 2. End-to-end delay Comparison

As shown in figure 2, the delay of the proposed technique is compared with existing technique. It is analysed that, proposed work during version number attack compared with existing work. It is identified from figure 2 that delay during the attack it is reduced around 17.66 % compared to the existing work.

The energy consumption is compared when the attack existing and proposed work. In comparisons, the proposed technique consumes the least amount of energy in the network and it is analysed that energy is reduced by 29.57 % as compared to the existing work as shown in figure 3.

As shown in figure 4, the comparisons are made on attack scenario of RPL and throughput impact during existing and proposed work. It is analysed that the proposed technique has maximum throughput as compared to other scenarios and throughput is increased by 11.03%.

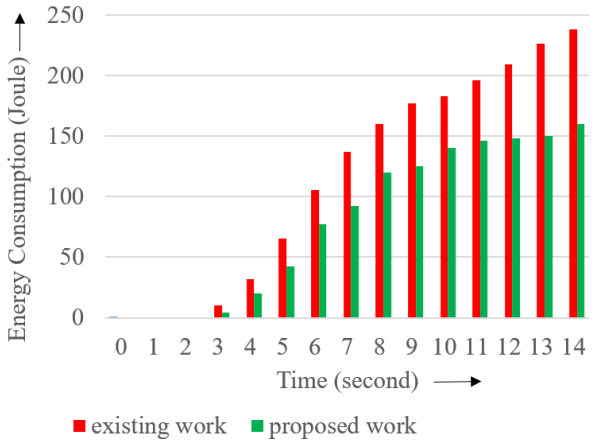

Figure 3. Energy Consumption

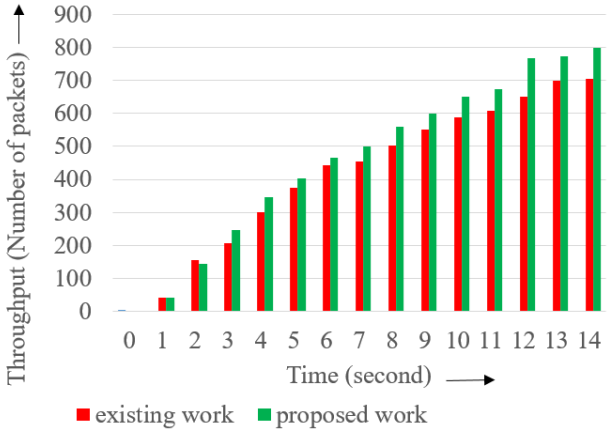

Figure 4. Throughput Comparison

Table 2. Packet Loss Ratio comparison

Execution Time (s)	No. of packet Receive	No of packet Loss		PLR	
		Existing work	Proposed work	Existing work	Proposed work
0	0	0	0	0.00	0.00
1	754	50	40	0.07	0.05
2	631	175	150	0.28	0.24
3	685	240	210	0.35	0.31
4	645	355	280	0.55	0.43
5	653	382	321	0.58	0.49
6	549	382	321	0.70	0.58
7	477	384	325	0.81	0.68
8	376	390	330	1.04	0.88
9	240	410	340	1.71	1.42
10	242	439	363	1.81	1.50
11	240	463	373	1.93	1.55
12	291	479	405	1.65	1.39
13	926	525	426	0.57	0.46
14	1018	535	450	0.53	0.44

The proposed technique is compared to the existing technique on PLR. A packet loss is described as a number of packet loss during the packet transitions. It is calculated by taking a ratio of the number of packet loss to the number of packets received. Table 2 presents a different time interval, the number of packets received, packet loss and their corresponding PLR for the existing and proposed method. From the analysis, it is identified that the proposed method has performed well and improve 16.93 % compared to the existing one.

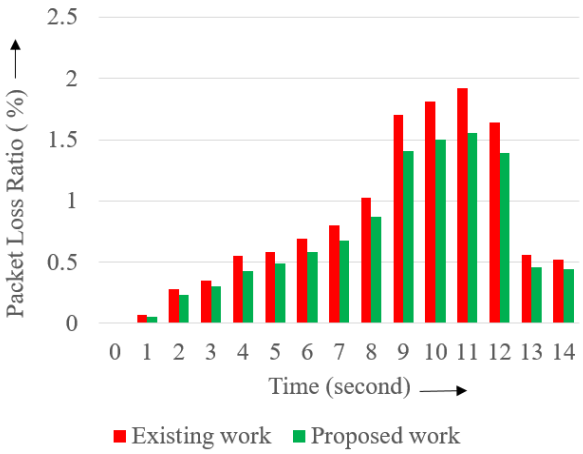

Figure 5. Packet Loss Ratio

A packet delivery ratio described as a number of packets successfully received to the total number of the transmitted packet. Table 3 presents a different time interval, the total number of the packet transmitted, a total number of packet received and their corresponding PDR for the existing and proposed method. From the analysis, it is identified that the proposed method has performed well and improve 12.19 % compared to the existing one.

Table 3. Packet Delivery Ratio comparison

Execution Time (s)	Total No Packet Transmitted	No of packet Received		PDR	
		Existing work	Proposed work	Existing work	Proposed work
0	0	0	0	0	0
1	804	754	764	0.94	0.95
2	806	631	656	0.78	0.81
3	925	685	715	0.74	0.77
4	1000	645	720	0.65	0.72
5	1035	653	714	0.63	0.69
6	931	549	610	0.59	0.66
7	861	477	536	0.55	0.62
8	766	376	436	0.49	0.57
9	650	240	310	0.37	0.48
10	681	242	318	0.36	0.47
11	703	240	330	0.34	0.47
12	770	291	365	0.38	0.47
13	1451	926	1025	0.64	0.71
14	1553	1018	1103	0.66	0.71

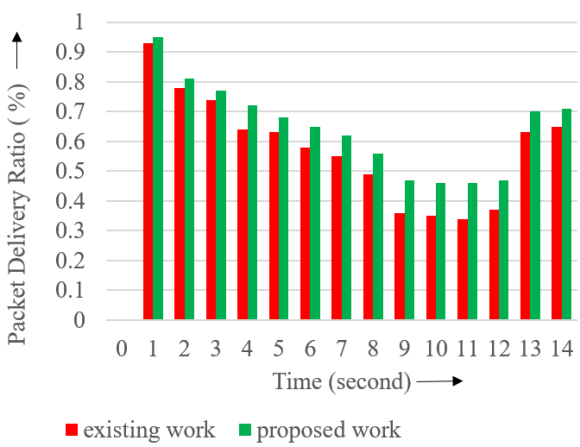

Figure 6. Packet delivery Ratio

VI. CONCLUSION

Internet of things is comprised of numerous numbers of nodes, communicating with each other. Which triggers the possibility of version number attack, affecting the performance of the IoT network in many ways. However, for our work, we have emphasized on delay, energy consumption, throughput, PLR and PDR. The proposed method uses monitoring of malicious activity based on threshold value to detect the version number attack. The node start to monitor the preserve of malicious node to isolate it from the path and improve the performance. The proposed technique is implemented in network simulator version 2 and results are analysed and compared with existing work in terms of end-to-end delay, energy consumption, PLR, PDR and throughput. It is analysed that in all three parameters proposed techniques perform well compared to the existing is in 17.66%, 29.57%, 16.93%, 12.19%, 11.03% respectively.

REFERENCES

[1] K.K. Patel, S.M. Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", International journal of engineering science and computing, vol. 6(5), 2016**.**

[2] O. Iova, P. Picco, T. Istomin, C. Kiraly, "RPL: The Routing Standard for the Internet of Things... Or Is It? ", IEEE Communications Magazine, vol. 54(12), pp. 16-22, 2016.

[3] F. Ahmed and Y.B. Ko, "A Distributed and Cooperative Verification Mechanism to Defend against DODAG Version Number Attack in RPL", Proceedings of the 6th International Joint Conference on Pervasive and Embedded Computing and Communication Systems, SCITEPRESS-Science and Technology Publications, Lda, 2016.

[4] G. Glissa, A. Rachedi, A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things", 2016 IEEE Global Communications Conference (GLOBECOM), Washington, pp. 1-7, 2016.

[5] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, IETF, 2012.

[6] D. Popa, N. Cam-Winget, J. Hui, "Applicability Statement for the Routing Protocol for Low Power and Lossy Networks (RPL) in AMI Networks", Internet Engineering Task Force, Internet-Draft draft-ietfroll-applicability-ami-13, work in Progress, 2016.

[7] A. Kamble, V.S. Malemath, D. Patil, " Security attacks and secure routing protocols in RPL-based Internet of Things: Survey" , 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 10.1109/ETIICT.2017.7977006, pp. 33-39, 2017.

[8] A. Baccelli, R. Cragie, P. Van, A. Brandt, "Applicability Statement: The Use of the Routing Protocol for Low-Power and Lossy Networks (RPL) Protocol Suite in Home Automation and Building Control", RFC 7733, 2016.

[9] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schonw , "A Study of RPL DODAG Version Attacks", IFIP international conference on autonomous infrastructure, management and security, Springer, Berlin, Heidelberg, 2014.

[10] A. Aris, S.F. Oktug, and S.B.O. Yalcin, "RPL Version Number Attacks: In-dept Study", NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, 2016.

[11] A. Dvir, T. Holczer, L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL", IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 709–714, 2011.

[12] H. Perrey, M. Landsmann, O. Ugus, M. Wahlisch, T.C. Schmidt, "TRAIL: Topology Authentication in RPL", arXiv preprint arXiv: 1312.0984, 2013.

[13] A. Le, J. Loo, Y. Luo, A. Lasebae, "Specification-based IDS for Securing RPL from Topology Attacks", IFIP Wireless Days (WD), Niagara Falls, Canada, pp. 1–3, 2011.

[14] S. Raza, L. Wallgren, T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", Ad Hoc Networks, vol. 11(8), pp. 2661–2674, 2013.

[15] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schonw, "Using the RPL Protocol for Supporting Passive Monitoring in the Internet of Things", NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 366-374, 2016.

[16] H. Patel , H.B. Patel, B. Shrimali, "A Survey on Trust-based Intrusion Detection for Version Number Attack on RPL", International Journal of Computer Sciences and Engineering (UGC recognized journal #63193, E-ISSN: 2347-2693) vol.6, Issue.10, 2018.

[17] A. Mayzaud, R. Badonnel, I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, vol. 18(3), pp.459-473, 2016.

[18] H.A. Abdul-Ghani, D. Konstantas M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model", (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 9(3), 2018.

[19] Z.A. Khan, P. Herrmann, "A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things", 2017 IEEE 31st International Conference on Advanced Information Networking and Applications, pp. 1169-1176, 2017.

[20] A Mayzaud, R. Badonnel, I. Chrisment, "Detecting Version Number Attacks in RPL-based Networks using a Distributed Monitoring Architecture", 12th International Conference on Network and Service Management (CNSM), pp. 127-135, 2016.

[21] H. Abdo, M. Kaouk, J-M. Flaus, F. Masse, "A safety/security risk analysis approach of industrial control systems: a cyber-bowtie - combining new version of attack tree with bowtie analysis", Computers & Security, vol. 72, pp. 175-195, 2017.

[22] D.J. Weller-Fahy, B.J. Borghetti, A.A Sodemann, "A survey of distance and similarity measures used within network intrusion anomaly detection", IEEE Communications Surveys & Tutorials, vol. 17(1), pp.70-91, 2015.

[23] M.A. Lodhi, A. Rehman, M.M. Khan, F.B. Hussain, "Multiple path RPL for low power lossy networks", 2015 IEEE Asia Pacific Conference on Wireless and Mobile, pp. 279-284, 2015.